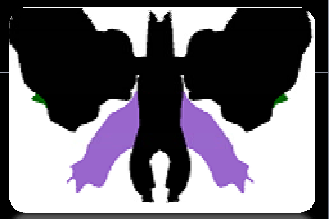
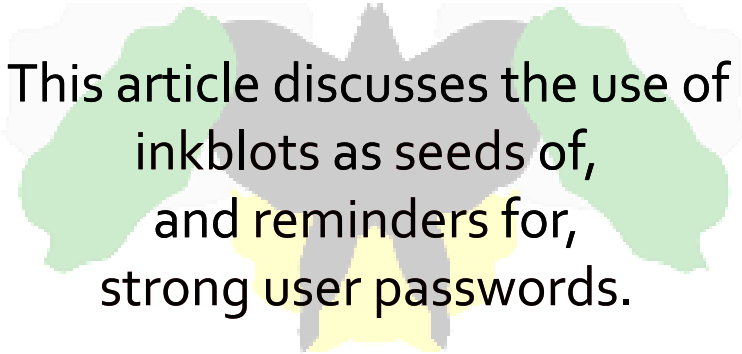
Inkblot Authentication



John Downs

A. Stubblefield, D. Simon, "Inkblot Authentication", Microsoft Research Technical Report MSR-TR-2004-85, 16 pp., August 2004. Available: ftp://ftp.research.microsoft.com/pub/tr/TR-2004-85.pdf, 4 August2008.

Article Summary



This article discusses the use of inkblots as seeds of, and reminders for, strong user passwords.

Pictorial Passwords
A Psychological Perspective

- Pictorial passwords a clever idea.
  - Inkblots seem to have good characteristics.
- "… humans can **remember** pictorial representations more readily than textual or verbal representations."
  - "Remember" - recognition vs. recall?
  - Not remembering pictures – they're presented to you!
  - Conceptual memory.
- No long-term analysis of memorability.

Integration with Existing Systems

- This mechanism could be added into other password systems relatively easily.
  - i.e. it doesn't alter the basic way passwords work.
  - Need to store the inkblot generation seeds.
  - User interface needs to be updated.
  - Could be componentised.
- Low cost of adoption and high gain in usability.

Password Security

- There may be common things that people will see in blots.
  - e.g. Batman.
- Frequency analyses can guide brute force attacks.
- People may be able to guess each other's responses.

And:

- The password is the same each time, so it could be compromised like a normal password.

Password Security

- So these passwords have a lot of the drawbacks of normal passwords, and have unique weak points as well.
- More secure than word-based passwords; less secure than random passwords.

- "We have attempted to design a scheme that… ensures that nearly every easily remembered password is secure."
- "Even mildly strong, highly memorable passwords are useful for some situations…"

What factors would make this more, less, or as secure as using a normal password?